ist, festgehalten, dass sie insgesamt gut gelungen sei. Sie hätten zwar als Betriebsrat auf bestimmte Regelungen verzichtet, dafür aber sehr viel mehr Möglichkeiten in der praktischen Gestaltung der Software-Einführung und -Nutzung erhalten. Teile der Vereinbarung seien außerdem so gestaltet, dass sie als Betriebsrat bei Bedarf die Regelungen einklagen könnten.

Die Stimmung in der Projektgruppe war gut und auf Einvernehmen ausgerichtet, wäre sie jedoch umgeschlagen, hätte man einige Vereinbarungen wörtlicher nehmen müssen.

Der Betriebsratsvorsitzende zieht das Resumee, dass es besonders wichtig sei, eine klare Zielsetzung zu verfolgen. Wenn sich alle Beteiligten grundsätzlich einig seien, dass das System zum Wohle des Unternehmens und der Mitarbeiter eingeführt wird, dann sei auch eine befriedigende betriebliche Einigung möglich.

Karl-Hermann Böker, freier Journalist und Technologieberater; Kontakt: Böker-Beratung, Hartlager Weg 61a, 33604 Bielefeld, fon 0521-9273 94-48; **post@khboeker.de**, **www.boeker-beratung.de**

Dieser Artikel stützt sich auf ein Interview, das der Autor mit den Vertretern des Paracelsus-Betriebsrats im April 2006 geführt hat.

***Kontakt zum Betriebsrat der Paracelsus-Klinik Osnabrück: fon 0541-966-3900, fax 0541-966-3901,* axel.denker@pk-mx.de; udo.muhle@pk-mx.de**

ULRICH MOTT

Dokumente unter Kontrolle

Mit der Digital-Rights-Management-Technik, angewandt auf Dokumente im Unternehmen, kann man Zugriffsberechtigungen sehr genau festlegen. Dies wird genutzt, um die Datensicherheit zu erhöhen. Gleichzeitig ergeben sich aber bisher unbekannte Möglichkeiten zur Leistungs- und Verhaltenskontrolle.

Digital Rights Management (DRM), also die Handhabung digitaler Rechte, wurde bisher hauptsächlich im Zusammenhang mit dem Herunterladen von Musik aus dem Internet bekannt. Mit dieser Technik kann die unerwünschte oder unerlaubte Weitergabe von gekauften Musikstücken an Dritte verhindert werden – ein Thema, das für die Betriebsrats- oder Personalratsarbeit eher wenig interessant ist.

Neuerdings kommen aber zunehmend Produkte zum Einsatz, die ähnliche Techniken für die Verwaltung von Dokumenten im Unternehmen anbieten. So hat Microsoft 2003 die *Rights-Management-Services* (RMS) herausgebracht und *Adobe* bietet für Dokumente im PDF-Format ⊡→ den *LiveCycle Policy Server* an, weitere Hersteller sind unter anderen *SealedMedia* und *Authentica*.

DRM-Funktionen bei der Dokumentenverwaltung

Wozu werden diese Produkte überhaupt benötigt, wo doch schon mit dem Betriebssystem *Windows* differenzierte Berechtigungen für Dateien vergeben können, von der Verwahrung und Verwaltung von Dokumenten in Dokumenten-Management-Systemen (siehe: *ECM – Achtung, da kommt was auf uns zu!* in cf 3/06 ab Seite 11) ganz abgesehen?

Nun, normalerweise kann jeder, der eine Datei lesen kann, sie auch an anderer Stelle abspeichern, kann sie verändern, ausdrucken oder via E-Mail weiterschicken. Außerdem können sich Systemadministratoren ⊡→ in der Regel den Zugriff zu allen Dateien beschaffen. Wenn man also verhindern will, dass zum Beispiel Konstruktionspläne an die Konkurrenz geschickt werden oder dass der Geschäftsbericht schon vor der offiziellen Veröffentlichung die Presse erreicht, muss man zusätzliche Maßnahmen ergreifen.

Auch das Lese-Kennwort, das gelegentlich benutzt wird, um beispielsweise bestimmte Text-Dokumente zu schützen, hilft nicht gegen den Missbrauch durch die Benutzer, die berechtigterweise das Kennwort wissen. Außerdem ist dies Verfahren unbrauchbar, wenn man sich vielleicht für 100 Dokumente 100 Kennworte merken müsste.

Diese Lücke soll nun durch DRM-Produkte geschlossen werden. Der Ablauf des dafür nötigen Verfahrens ist – stark vereinfacht – etwa dieser (siehe auch Abbildung oben):

1. Schritt: Der Autor eines Dokuments entscheidet, dass dieses Dokument geschützt werden soll und er legt Zugriffsberechtigungen fest. Demnach darf zum Beispiel Herr Meiering das Dokument lesen, ausdrucken und weiterleiten, die Mitglieder der Gruppe ›Verkauf‹ hingegen dürfen es nur am Bildschirm anzeigen und ändern darf es niemand. Es ist also die Vergabe sehr differenzierter Berechtigungen möglich. So kann man auch festlegen, ob der Empfänger Inhalte kopieren kann oder dass das Dokument an einem bestimmten Datum ungültig und damit für alle Benutzer gesperrt wird. Diese verschiedenen Einstellungen werden an das Dokument angefügt und dann wird alles verschlüsselt.

2. Schritt: Der Autor verteilt das Dokument, zum beispiel als E-Mail, auf CD oder er stellt es irgendwo im Netzwerk zur Verfügung.

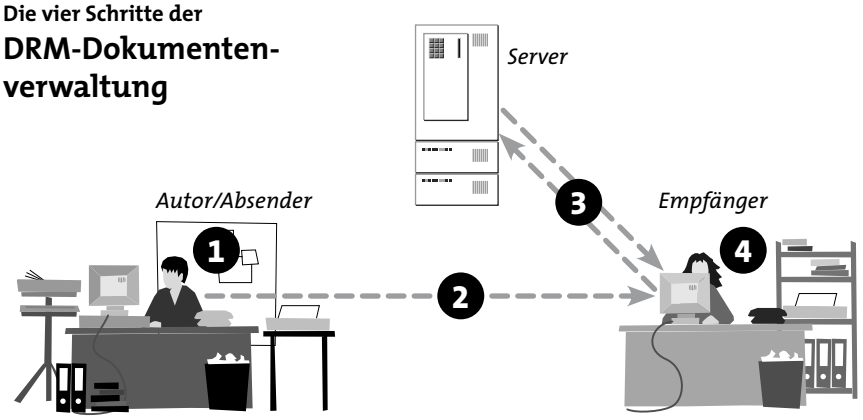
3. Schritt: Wenn der Empfänger auf das Dokument zugreifen will, stellt sein Programm eine Verbindung zu einem zentralen Server ⊡→ her und schickt die an das Dokument angehängten Berechtigungseinstellungen dorthin. Der Server prüft, ob die Berechtigungen noch aktu-

ell sind (der Autor könnte es sich ja in der Zwischenzeit anders überlegt und eine Sperrmitteilung verschickt haben) und liefert dem Empfänger den notwendigen Schlüssel zum Öffnen des Dokuments.

4. Schritt: Auf dem Rechner des Empfängers wird das Dokument automatisch entschlüsselt und das Programm sorgt dafür, dass der Empfänger nur die vorgesehenen Aktionen durchführen kann.

Benötigt wird für dieses Rechte-Management neben einem Server, der die Identität des Empfängers prüft, die nötigen Schlüssel zur Verfügung stellt und Änderungen verwaltet, nur noch eine entsprechende Software auf dem Rechner des Benutzers. Im Fall der am weitesten verbreiteten Büro-Programme von Microsoft ist das Softwarepakte *Office 2003* dafür schon vorbereitet. Und auch bei Adobe, dem Marktführer bei der PDF-Technik, können die Programme *Acrobat* und *Acrobat Reader* diese Funktionen bereits ausführen. Andere DRM-Hersteller liefern Zusätze für ihre Produkte zu den gängigen *Office*-Programmen.

Die vier Schritte der
DRM-Dokumenten-verwaltung



Leistungs- und Verhaltens-kontrolle ist möglich

Da beim digitalen Rechte-Management jeder Zugriff auf ein Dokument an einer zentralen Stelle, dem Server, freigegeben werden muss, kann man den Zugriff dort auch gleich festhalten. In der Tat verfügen alle diese Produkte über umfangreiche Protokollierungsfunktionen. Damit kann man nicht nur verfolgen, wer wem welche Dokumente weitergeleitet hat – was ja bei vertraulichen Unterlagen durchaus sinnvoll sein kann –, sondern jede Aktion eines Benutzers kann protokolliert werden.

Dabei kann schon das Lesen eines Dokuments (eine Tätigkeit, die man normalerweise bisher tun konnte, ohne Spuren zu hinterlassen) einen Protokolldatensatz erzeugen. Und bei einigen Systemen ist dieses Protokoll nicht nur für die Administratoren, sondern auch für den Autor eines Dokuments zugänglich. Auch eine Benachrichtigung des Autors ist möglich, wenn der Empfänger das Dokument öffnet – oder wenn er es nach 24 Stunden immer noch nicht geöffnet hat. Für bestimmte Vorgänge mag selbst das sinnvoll sein, es ist aber auch eine gezielte Verhaltenskontrolle denkbar.

Auf jeden Fall sollte ein Betriebsrat oder Personalrat bei der Einführung eines solchen Systems also sein Mitbestimmungsrecht wahrnehmen und den Umfang der Protokollierung regeln.

DRM = Sicherheit für Betriebs-/ Personalrats-Dateien?

Stellt sich zum Schluss noch die Frage: Wenn ein solches System eingeführt wird, könnte der Betriebsrat es zum Schutz der eigenen Dokumente nutzen? Mit Vorbehalt. Denn, wie so häufig, gibt es doch jemanden, der die geschützten Dokumente mit einem ›Generalschlüssel‹ wieder entschlüsseln kann: der Administrator dieses Systems. Um Dokumente von ausgeschiedenen Mitarbeitern weiter nutzen zu können, kann dieser Generalschlüssel hilfreich sein, für den Betriebs- oder Personalrat – oder vielmehr für seine Dateien – ist er jedoch eine mögliche Gefahr. Nur wenn man eine Funktionstrennung realisiert, bei der zum Beispiel der Windows-Administrator keine DRM-Rechte hat und der DRM-Administrator keine Windows-Zugriffsberechtigungen, kann man sichere Lösungen erreichen.

Und noch eine Schwierigkeit gibt es: Wenn die Dateizugriffsrechte an Gruppen vergeben werden und das DRM-System dabei auf die im Betriebssystem angelegten Benutzergruppen zurückgreift, könnte sich ein Windows-Administrator heimlich zum Mitglied der Gruppe Betriebsrat machen und damit auf alle Dokumente des Betriebsrats zugreifen.

Ob man einer solchen Lösung vertraut, hängt also wieder davon ab, ob die Administration vernünftig organisiert ist – oder ob man den Administratoren vertrauen kann.

Ulrich Mott ist Berater bei FORBIT; Kontakt: FORBIT GmbH, Eimsbütteler Straße 18, 22769 Hamburg, fon 040-432 25 67, **http://forbit.de**, **mott@forbit.de**

Server (Zusteller) = spezielle Rechner oder auch Software, die dafür zuständig sind, innerhalb eines Netzwerks Daten oder auch Programme für die angeschlossenen Rechner (Clients) zu Verfügung zu stellen und Netzwerkfunktionen zu steuern und zu verwalten oder bestimmte ›dienste‹ zu verrichten (z.B. die Steuerung einer Telekommunikationsanlage oder des E-Mail-Verkehrs)

Systemadministrator = Verwalter, Einrichter und Betreuer von Computersystemen und -netzwerken

PDF (Portable Document Format) = Technik, mit der Dokumente aus verschiedensten Programmen so umgewandelt werden, dass sie auf anderen Computern gelesen werden können, ohne dass diese über das Programm verfügen müssen, mit dem das Dokument erstellt wurde